(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 805 610 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.11.1997 Bulletin 1997/45

(51) Int Cl.[6]: **H04Q 7/38**

(21) Application number: **97303041.4**

(22) Date of filing: **02.05.1997**

(84) Designated Contracting States:
DE FR GB SE

(30) Priority: **02.05.1996 US 641841**

(71) Applicant: **NOKIA MOBILE PHONES LTD.**
02150 Espoo (FI)

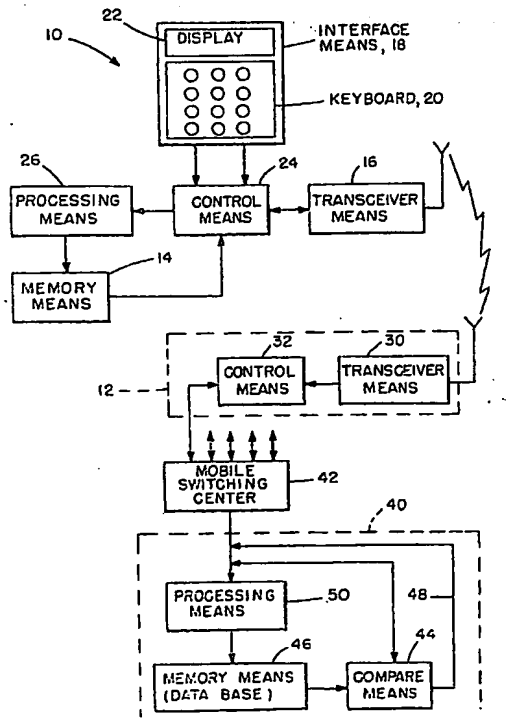
(72) Inventor: **Hosseini, Walid**
San Diego, California 92122 (US)

(74) Representative: **Potter, Julian Mark et al**
Nokia Mobile Phones,
Patent Department,
St. Georges Court,
St. Georges Road,
9 High Street
Camberley, Surrey GU15 3QZ (GB)

(54) Method and system for detection of fraudulent cellular telephone use

(57) A system to detect the use of stolen mobile identification number (MIN) and electronic serial number (ESN) information to fraudulently place wireless calls by comparing the last phone number connected (LNC) as recorded by the radio telephone network (40) with the last phone number connected as recorded in the mobile radio telephone unit (10). The mobile radio telephone unit LNC is transmitted to the base station (12) upon initiation of a radio telephone call for comparison with the LNC recorded by the radio telephone network (40). The network will detect if a MIN/ESN combination is in use by two different mobile units because the LNC of the two mobile units (10) will be different due to the different phone numbers called by each user.

FIG. 1.



EP 0 805 610 A2

Description

The present invention relates to radio telephones, and more particularly to apparatus and method to detect and/or prevent unauthorized and fraudulent use of the radio telephone.

Wireless, radio telephones such as mobile phones are identified by a unique mobile identification number (MIN) and a unique electronic serial number (ESN). Both these identifying characteristics are transmitted over the air between the mobile phone and the telephone systems mobile switching center, and are therefore able to be obtained by scanning equipment and illegally used in another (clone) phone with the cost being charged to the owner of the original phone.

A prior proposed solution to the illegal usage is to monitor the calling patterns for each customer's wireless calls and to block any calls that do not correspond to the customer's prior calling pattern. However, this solution may result in the blocking of calls for an authorized customer if they change their calling pattern, and it will not successfully block calls from phones that continually change the MIN-ESN that they use (so-called "tumbler-cloner" or "Magic phones". Also, typically the calling pattern can only be checked after the call is completed, at which time it is too late to prevent the fraud.

Another prior solution to the problem is to utilize the IS 54 B Cellular System Dual-Mode Mobile Station -- Base Station Compatibility Standard (Rev-B). The IS 54 B standard calls for pre-call authentication of the calling wireless telephone using a "shared secret key" over a digital call set-up channel. A shared secret key is a key that is known only by the two parties involved in the authentication. This proposed solution suffers from the problems that in order to be operative it requires both cooperation and investment on the part of all the wireless carriers, such as the ability to access each other's data bases where the keys are stored and upgrading of their switching equipment to be compatible with the IS 54 B call set standard. These propositions are computationally intensive, expensive and require a long time to implement.

Still another solution is the technique described in U.S. Patent 5,420,908 issued May 30, 1995 to Hodges et al. entitled METHOD AND APPARATUS FOR PREVENTING WIRELESS FRAUD. In the Hodges et al. patent the use of stolen mobile identification number (MIN) and electronic serial number (ESN) information to fraudulently place wireless calls is prevented by having the switches of multiple wireless carriers forward or direct, over a telephone connection, all calls placed from selected MINs to a central authentication platform that serves the multiple wireless carriers. The central authentication platform engages in a so-called "challenge-response" authentication with local processors that are interfaced to the wireless telephones from which non-fraudulent calls originate. The challenge-response authentication uses a shared secret key (S-Key) that is not broadcast over the air interface, thus preventing the key from being "stolen". A call from a wireless telephone that is not interfaced to a local processor capable of successfully completing the challenge-response authentication is completed to the number desired by the customer. Advantageously, since the central authentication platform serves multiple wireless carriers, the need for one wireless carrier to access the database of another is alleviated and the expense of providing additional security is reduced.

The Hodges et al. technique is another example of a "shared secret data" technique that involves intensive compilation and relies on encryption techniques having algorithms that must be maintained secret.

In the present invention, the use of stolen mobile identification number (MIN) and electronic serial number (ESN) information to fraudulently place wireless calls is detected by comparing the last phone number connected (LNC) as recorded by the radio telephone network with the last phone number connected as recorded in the mobile radio telephone unit. The mobile unit LNC is transmitted to the base station upon initiation of a radio telephone call for comparison with the LNC recorded by the radio telephone network. The network will detect if a MIN/ESN combination is in use by two different mobile units because the LNC of the two mobile units will be different due to the different phone numbers called by each user. This method provides an advantage that no secret keys are needed, the effective signature of a mobile unit changes with each phone call made, and detection of fraudulent use is available within a few phone calls.

According to one aspect of the present invention, there is provided a detection system for detecting the unauthorized use of a mobile radio telephone unit comprising:

at least one mobile radio telephone unit including:

a first memory means for storing first numeric data representative of a last number connected (LNC);

a first transceiver means for receiving and transmitting radio telephone communications;

a first control means;

a user interface means connected to said first control means for inputting a telephone number by a user;

said first control means coupled to said first transceiver means for making and receiving radio telephone calls, and transmitting said inputted telephone number from said user interface means, said first control means further coupled to said first memory means for recalling and transmitting said first numeric data representing a last telephone number

connected (LNC) and stored in said first memory means;

a first processing means coupled to said first control means and to said first memory means for and responsive to said inputted telephone number from said user interface means and stored in said first memory means to form said first numeric data (LNC) representing a last number connected each time a radio telephone call occurs;

a radio telephone network including

at least one base stating including

a second transceiver means for receiving and transmitting radio telephone communications;

a second control means to coupled to said second transceiver means for making and receiving radio telephone calls, said second control means further receiving from said second transceiver means said inputted telephone number and said first numeric data (LNC) transmitted from said at least one mobile radio telephone unit and received by said second transceiver means;

a network communication means, coupled to said second control means, for connecting said at least one base station to said radio telephone network, said network communication means including;

a second memory means for storing second numeric (LNC) data;

a comparing means coupled to said second memory means and to said second control means for comparing said second numeric (LNC) data stored and said first numeric data (LNC) received to generate a comparison signal;

a second processing means coupled to said second control means and to said second memory means and responsive to said inputted telephone number received from said at least one mobile radio telephone unit to form said second numeric data (LNC) which is stored in said second memory means each time a radio telephone call occurs

wherein unauthorized use of said at least one mobile radio telephone unit is indicated by said comparison signal when said second numeric data (LNC) stored in said network communication means is not the same as said first numeric data (LNC) received from said at least one mobile radio telephone unit when a radio telephone call occurs.

According to another aspect of the present invention, there is provided a method of detecting the unauthorized use of a mobile radio telephone comprising:

receiving at a mobile radio telephone network communications center a request for wireless telephone communication from a mobile radio telephone unit said request including a particular mobile identification number (MIN) data and electronic serial number (ESN) data for the mobile unit and last number connected (LNC) data from the mobile unit,

receiving from the mobile unit a telephone number entered by a user;

comparing said LNC data received from the mobile unit with LNC data previously stored in the network communications center for the mobile unit having said particular MIN/ESN data;

responding to a difference indicated by the comparison of said LNC received and said LNC stored to indicate an unauthorized use of said mobile units.

The present invention provides an apparatus and method that uses not only the MIN and ESN but also the last number connected (LNC) by the mobile unit.

Previous fraud detection techniques are static. Once the ESN of a legitimate mobile has been stolen, the original phone has been virtually cloned with no possibility of detection until the customer receives his or her bill.

The present invention provides a dynamically updated system of identifying a mobile. The dynamic variable is simply the last number which was dialed for which a phone call was completed by the mobile. This information is readily available both to the mobile and the base station. More significantly, it is ever changing through the regular use of the phone.

In operation, when an attempt is made by a mobile to access the system, the system would not only ask for the usual MIN/ESN combination, but also for the last number the phone dialed and connected (LNC). An intruder may manage to steal this information over the air, at the same time he steals the ESN/MIN. However, he now may only use this combination for as long as the original, legitimate user, does not make another call. Furthermore, as soon as the intruder has made a call, the first call placed by the legitimate user would trigger detection of dual usage of the same ESN. The course of action at this point could vary in severity from covert observation and localization of the intruder to outright termination of the service with a message indicating the cause of the termination. The legitimate user would probably be grateful for not having to go through the process of proving that the several thousand dollars showing up on his bill are fraudulent, while the intruder would suffer the shock of having been detected.

Other and further features, advantages and bene-

fits of the invention will become apparent in the following description taken in conjunction with the following drawings. It is to be understood that the foregoing general description and the following detailed description are exemplary and explanatory but are not to be restrictive of the invention.

The accompanying drawings which are incorporated in and constitute a part of this invention and, together with the description, serve to explain the principles of the invention in general terms.

In the drawings:

Fig. 1 is a schematic illustration of a system for the detection of fraudulent use of a wireless radio telephone according to the principles of the present invention.

Figs. 2 and 3 are illustrations of flow charts for a method of fraud detection in wireless radio telephone systems according to the principles of the present invention.

Referring to Fig. 1, an illustration of an embodiment of a system for the detection of fraudulent use of a wireless telephone is provided including a mobile radio telephone system. The mobile radio telephone system comprises at least one mobile unit 10 including a memory means 14 for storing numeric data signal, a transceiver means 16 for receiving and transmitting radio telephone communication signals, a user interface means 18 including a keypad 20 for inputting a telephone number and a display means 22 for displaying telephone numbers and other messages, and a control means 24 coupled to the user interface means 18. The control means 24 is also coupled to the transceiver means 16 for making and receiving radio telephone calls, and for transmitting the present telephone number that the user input. The control means 24 is further coupled to the memory means 14 for recalling and transmitting a numeric data signal which represents the last telephone number dialed and connected (LNC) and which is stored in the memory means 14. Memory means 14 also has stored in it the MIN and ESN for the mobile unit 10, and the MIN and ESN is also transmitted along with the numeric data signal.

A processing means 26 is coupled to the control means 24 and to the memory means 14 for manipulating an input telephone number to form the numeric data signal which represents the last number connected and which is stored in the memory means 14 each time a radio telephone call occurs. The at least one mobile unit 10 is connected through an air interface to at least one base station 12 that includes a transceiver means 30 for receiving and transmitting radio telephone communication signals and a control means 32 coupled to transceiver means 30 for making and receiving radio telephone calls. The control means 32 further receives, from the transceiver means 30, the input telephone number and the numeric data signal (i.e. LNC) transmitted by the mobile unit 10 and received by the transceiver means 30 of base station 12 along with the MIN and ESN. An optional mobile switching center 42 is coupled to the base station for interconnecting it to all base stations in the system. A network communications center 40 is provided, which may be located remote from base station 12, for example, by being connected to mobile switching center 42. Network communications center 40, includes a memory means 46 for storing a numeric data signal, a comparing means 44 is coupled to memory means 46 and also coupled to the base station, for example via mobile switching center 42 for comparing the numeric data signal (LNC) stored in memory means 46 and the numeric data signal (LNC) transmitted by memory means 14 of mobile unit 10 to generate a comparison signal on output 48. A processing means 50 is also coupled to control means 32 via mobile switching center 42 and to memory means 46 for manipulating the input telephone number received in a radio telephone communication from the mobile unit 10 to form a new or updated numeric data signal (LNC) which is stored in memory means 46 each time a radio telephone call occurs. An unauthorized use is indicated by the comparison signal produced when the numeric data signal (LNC) stored in memory means 46 of the network communications center 40 is not the same as the numeric data signal (LNC) received from the memory means 14 of mobile unit 10 via base station 12 when a radio telephone call occurs.

When the output of comparing means 44 indicates that the two numeric data signals are not the same, the telephone call can be terminated or can be permitted to continue as desired.

Referring to Fig. 2, a flow chart illustrates the steps of the method for carrying out the present invention.

Referring to Fig. 2, an overview of the steps of the inventive method is presented in the flow chart.

In block 60 the step of originating the mobile telephone call is performed. Then, in block 62, the step of fraud detection and updating the system parameters is carried out. Novel steps of the present invention are carried out essentially in block 62. After the step of block 62 has been performed either the conversation is permitted to take place over the mobile phone (block 64) or, optionally, the call is terminated (block 66).

If the conversation takes place according to block 64, at the conclusion of the conversation the call ends (block 68).

More particularly, Fig. 3 illustrates novel steps of the present invention. In the step of block 70 the fraud detection command is initiated. Then in the step of block 72 the mobile phone transmits the electronic serial number (ESN), the mobile identification number (MIN) and the last number connected (LNC) data to the base station transceiver means 30 of Fig. 1. In block 74 the mobile phone transmits the dialed number to the base station transceiver means 30 of Fig. 1. The ESN and the MIN are confirmed by the network communications center 40 and compare means 44 of Fig. 1 as shown in block 76 and the compare means 44 of network communications center 40 compares, as shown in block 78,

the LNC received from the mobile phone with the LNC stored in the network data base in memory means 46 of Fig. 1.

If there is no match between the LNC received from the mobile phone unit 10 and the LNC from the data base of memory means 46, then the "fraud detected" step of block 80 is carried out and, optionally, the call may be terminated (block 82) or proceed to complete the call (block 84).

If there is a match between the LNC from the mobile phone unit 10 and the LNC from the data base of memory means 46, then the "complete the call" step of block 84 is carried out.

In block 86, the data base stored in memory means 46 is updated with the LNC of the dialed number transmitted from mobile phone unit 10 in block 74.

Thus, upon the occurrence of another use of the mobile phone unit 10 with a new dialed number, the previously dialed (connected) number is now the LNC stored in the data base of memory means 46.

While the invention has been described in connection with a preferred embodiment, it is not intended to limit the scope of the invention to the particular form set forth, but, on the contrary, it is intended to cover such alternatives, modifications, and equivalence as may be included within the scope of the invention as defined in the appended claims.

Claims

1. A detection system for detecting the unauthorized use of a mobile radio telephone unit comprising:

at least one mobile radio telephone unit (10) including:

a first memory means (14) for storing first numeric data representative of a last number connected (LNC);

a first transceiver means (16) for receiving and transmitting radio telephone communications;

a first control means (24);

a user interface means (18) connected to said first control means (24) for inputting a telephone number by a user;

said first control means (24) coupled to said first transceiver means (16) for making and receiving radio telephone calls, and transmitting said inputted telephone number from said user interface means (18), said first control means (24) further coupled to said first memory means (14) for recalling and transmitting said first numeric data representing a last telephone number connected (LNC) and stored in said first memory means (14);

a first processing means (26) coupled to said first control means (24) and to said first memory means (14) for and responsive to said inputted telephone number from said user interface means (18) and stored in said first memory means (14) to form said first numeric data (LNC) representing a last number connected each time a radio telephone call occurs;

a radio telephone network including

at least one base station (12) including

a second transceiver means (30) for receiving and transmitting radio telephone communications;

a second control means (32) coupled to said second transceiver means (30) for making and receiving radio telephone calls, said second control means (32) further receiving from said second transceiver means (30) said inputted telephone number and said first numeric data (LNC) transmitted from said at least one mobile radio telephone unit (10) and received by said second transceiver means (30);

a network communication means (40), coupled to said second control means (32), for connecting said at least one base station (12) to said radio telephone network, said network communication means (40) including;

a second memory means (46) for storing second numeric (LNC) data;

a comparing means (44) coupled to said second memory means (46) and to said second control means (32) for comparing said second numeric (LNC) data stored and said first numeric data (LNC) received to generate a comparison signal;

a second processing means (50) coupled to said second control means (32) and to said second memory means (46) and responsive to said inputted telephone number received from said at least one mobile radio telephone unit (10) to form said second numeric data (LNC) which is stored in said second memory means (50) each time a radio telephone call occurs;

wherein unauthorized use of said at least one mobile radio telephone unit (10) is indicated by said comparison signal when said second nu-

meric data (LNC) stored in said network communication means (40) is not the same as said first numeric data (LNC) received from said at least one mobile radio telephone unit (10) when a radio telephone call occurs.

2. A detection system according to claim 1 wherein said radio telephone network includes a plurality of said base stations (12) and a mobile switching center means (42) coupled to said second control means (32) of each of said base stations for connecting said plurality of base stations (12) to each other.

3. A detection system according to claim 1 or 2 wherein said detection system includes a plurality of said mobile radio telephone units (10) each having stored therein separate, unique mobile identification number (MIN) data and electronic serial number (ESN) data, and wherein said MIN and ESN data is transmitted with said first numeric data (LNC).

4. A detection system according to any preceding claim, wherein said user interface (18) includes an alpha-numeric keypad (20) for inputting said telephone number by said user and a display means (22) for displaying alpha-numeric messages including telephone numbers.

5. A detection system according to any preceding claim further including means responsive to the output of said comparing means (44) for terminating said radio telephone call when said second numeric data (LNC) stored is not the same as said first numeric data (LNC) stored.

6. A method of detecting the unauthorized use of a mobile radio telephone (10) comprising:

receiving at a mobile radio telephone network communications center (40) a request for wireless telephone communication from a mobile radio telephone unit (10) said request including a particular mobile identification number (MIN) data and electronic serial number (ESN) data for the mobile unit (10) and last number connected (LNC) data from the mobile unit (10),

receiving from the mobile unit (10) a telephone number entered by a user;

comparing said LNC data received from the mobile unit (10) with LNC data previously stored in the network communications center (40) for the mobile unit (10) having said particular MIN/ESN data;

responding to a difference indicated by the comparison of said LNC received and said LNC stored to indicate an unauthorized use of said mobile units (10).

7. A method of detecting the unauthorized use of a mobile radio telephone unit according to claim 6 further including, upon indication of authorised use;

processing, in the network communications center (40), said telephone number entered by the user and received from said mobile unit (10) to create a new LNC data;

storing, in the network communications center (40), said new LNC data created from the telephone number entered by the user and received from said mobile unit;

processing in said mobile unit (10) the telephone number entered by said user to create said new LNC data;

storing in the mobile unit the new LNC data created from the telephone number entered by the user.

8. A method of detecting the unauthorized use of a mobile radio telephone unit according to claim 6 or 7 wherein comparing the LNC data received from the mobile unit with that previously stored in the network communications center (40) further includes confirming the validity of the mobile identification number (MIN) data and the electronic number (ESN) data received from said mobile unit.

9. A method as claimed in any of claims 6 to 8, further comprising:

terminating a call upon detection of an unauthorised use.

10. A system for detecting the unauthorised use of the mobile identification number (MIN) and electronic serial number (ESN) of a radiotelephone (10), the system comprising:

a radiotelephone (10) which transmits data representative of its last number connected (LNC) along with a call request; and

a network communications center (40) for receiving the call request, and which comprises:

means (46) for storing the LNC data for each MIN and ESN; and

means (44) for comparing the LNC data from the radiotelephone (10) with the LNC data for

the given ESN and MIN and indicating unauthorised use if they differ.

11. A radio communications switching system for detecting the unauthorised use of the mobile identification number (MIN) and electronic serial number (ESN) of a radiotelephone (10), the system comprising:

a receiver (30) for receiving a call request from a radiotelephone (10), the call request including data representative of the last number connected (LNC) to that radiotelephone (10);

means (46) for storing the LNC data for each MIN and ESN; and

means (44) for comparing the LNC data from the radiotelephone (10) with the LNC data for the given ESN and MIN and indicating unauthorised use if they differ.

12. A method of detecting unauthorised use of the mobile identification number and electronic serial number of a radiotelephone (10), the method comprising:

forwarding a call request from the radiotelephone (10) to a network communications center (40), the call request including the radiotelephone's (10) MIN, ESN and LNC data; and

comparing the LNC data from the radiotelephone (10) with LNC data stored in network communications center (40) for the particular ESN and MIN and determining unauthorised use if the data differs.

FIG. 1.

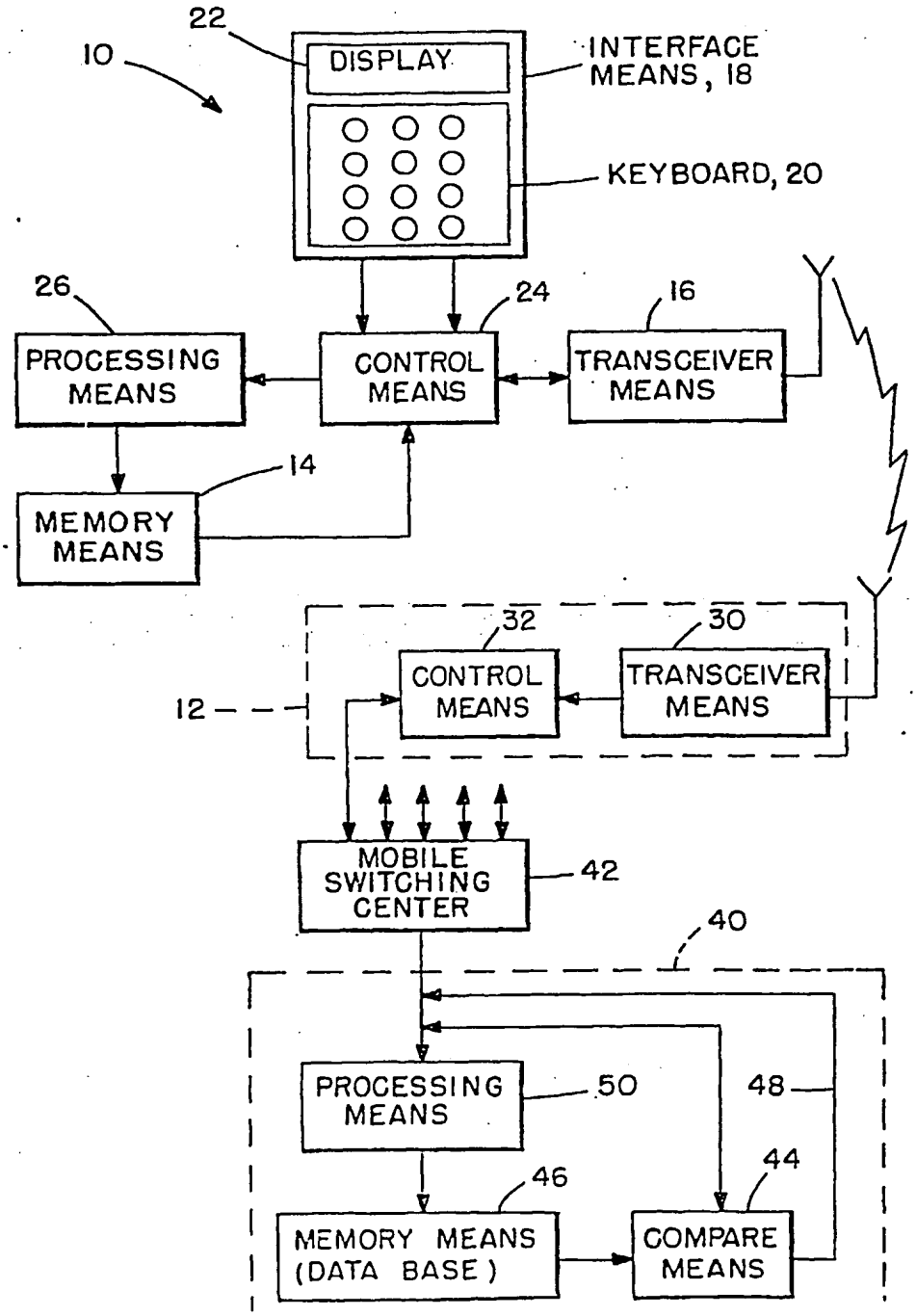

22
10
DISPLAY
INTERFACE MEANS, 18
KEYBOARD, 20
26
24
16
PROCESSING MEANS
CONTROL MEANS
TRANSCEIVER MEANS
14
MEMORY MEANS
32
30
12
CONTROL MEANS
TRANSCEIVER MEANS
MOBILE SWITCHING CENTER
42
40
PROCESSING MEANS
50
48
44
46
MEMORY MEANS (DATA BASE)
COMPARE MEANS

FIG. 2.

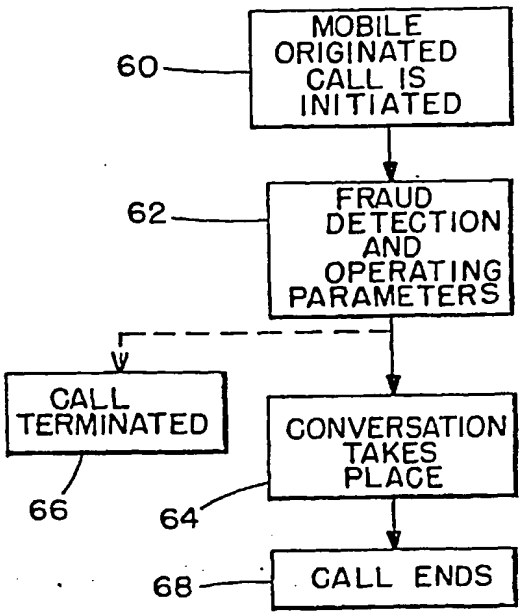
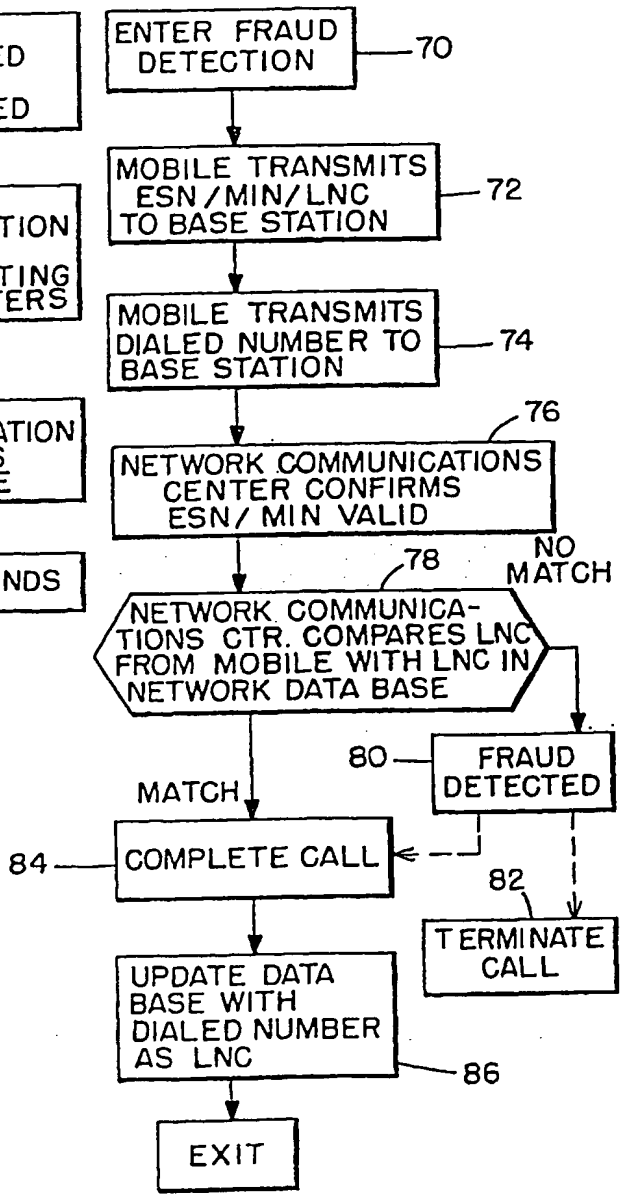

MOBILE ORIGINATED CALL IS INITIATED
60
FRAUD DETECTION AND OPERATING PARAMETERS
62
CALL TERMINATED
66
CONVERSATION TAKES PLACE
64
CALL ENDS
68

FIG. 3.


ENTER FRAUD DETECTION
70
MOBILE TRANSMITS ESN/MIN/LNC TO BASE STATION
72
MOBILE TRANSMITS DIALED NUMBER TO BASE STATION
74
NETWORK COMMUNICATIONS CENTER CONFIRMS ESN/MIN VALID
76
NETWORK COMMUNICATIONS CTR. COMPARES LNC FROM MOBILE WITH LNC IN NETWORK DATA BASE
78
NO MATCH
80
FRAUD DETECTED
MATCH
84
COMPLETE CALL
82
TERMINATE CALL
UPDATE DATA BASE WITH DIALED NUMBER AS LNC
86
EXIT

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 805 610 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
21.07.1999 Bulletin 1999/29

(43) Date of publication A2:
05.11.1997 Bulletin 1997/45

(21) Application number: **97303041.4**

(22) Date of filing: **02.05.1997**

(51) Int Cl.[6]: **H04Q 7/38**

(84) Designated Contracting States:
DE FR GB SE

(30) Priority: **02.05.1996 US 641841**

(71) Applicant: **NOKIA MOBILE PHONES LTD.**
02150 Espoo (FI)

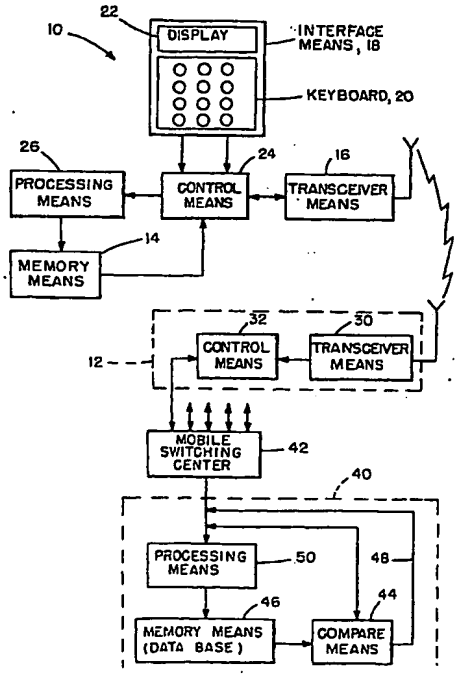
(72) Inventor: **Hosseini, Walid**
San Diego, Caligornia 92122 (US)

(74) Representative: **Potter, Julian Mark et al**
Nokia Mobile Phones,
Patent Department,
St. Georges Court,
St. Georges Road,
9 High Street
Camberley, Surrey GU15 3QZ (GB)

(54) Method and system for detection of fraudulent cellular telephone use

(57) A system to detect the use of stolen mobile identification number (MIN) and electronic serial number (ESN) information to fraudulently place wireless calls by comparing the last phone number connected (LNC) as recorded by the radio telephone network (40) with the last phone number connected as recorded in the mobile radio telephone unit (10). The mobile radio telephone unit LNC is transmitted to the base station (12) upon initiation of a radio telephone call for comparison with the LNC recorded by the radio telephone network (40). The network will detect if a MIN/ESN combination is in use by two different mobile units because the LNC of the two mobile units (10) will be different due to the different phone numbers called by each user.

FIG. 1.



EP 0 805 610 A3

Printed by Jouve, 75001 PARIS (FR)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 30 3041

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	US 4 955 049 A (GHISLER WALTER) 4 September 1990 * abstract * * column 2, line 32 - line 60 *	1,6,10, 12	H04Q7/38
A	US 5 457 737 A (WEN JACK C) 10 October 1995 * column 1, line 55 - column 2, line 45 *	1,6,10, 12	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	2 June 1999	Dionisi, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 97 30 3041

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

02-06-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4955049 A	04-09-1990	SE 500289 C	30-05-1994
		CA 1309466 A	27-10-1992
		SE 8902715 A	12-02-1991
US 5457737 A	10-10-1995	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82